UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/765,417	01/27/2004	Fujio Watanabe	M-15391 US	2223

32605 7590 04/14/2009

Haynes and Boone, LLP
IP Section
2323 Victory Avenue
SUITE 700
Dallas, TX 75219

EXAMINER	
PATEL, NIRAV B	

ART UNIT	PAPER NUMBER
2435	

MAIL DATE	DELIVERY MODE
04/14/2009	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/765,417	WATANABE ET AL.	
	Examiner	Art Unit	
	NIRAV PATEL	2435	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *11 March 2009*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-64* is/are pending in the application.

4a) Of the above claim(s) *34-54 and 56-63* is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-33,55 and 64* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. This action is in response to the communication filed on 11/20/2006.

2. Claims 1-64 are pending. Applicant's election without traverse of the elected group Species I, Claims 1-27, 28-33, 55, 64, in the reply filed on 3/11/09 is acknowledged. Claims 34-40, 41-48, 49-52, 53, 54, 56-62, 63 are drawn to nonelected species, thus withdrawn from further consideration.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

3. Claims 1-33, 55, 64 are rejected under 35 U.S.C. 103(a) as being unpatentable over Y. Choi and S. Pack, "Fast Inter-AP Handoff Using Predictive Authentication Scheme in a Public Wireless Network." (hereafter "Choi") in view of Faccin et al (US Patent No. 6,876,747) and in view of Palekar et al (US Pub. No. 2003/0226017).

As per claim 1, Choi teaches: A method for handoff in a wireless communication network, comprising: generating a handoff encryption key [Page 1, Introduction, Lines 11-14, page 6-7, 3.2, Fig. 5, 6]; handing off a wireless terminal from a first access point to a second access point [Page 1, Introduction, Lines 11-14, page 6-7, 3.2, Fig. 5, 6]; communicating data packets encrypted with the handoff encryption key between the

second access point and the wireless terminal [page 6-7, 3.2, Fig. 5, 6]. Choi teaches the authentication of the wireless terminal with an authentication server [Fig. 5].

Choi doesn't expressively mention immediate secure data transmission before the authentication of the wireless terminal is completed.

Faccin teaches communicating data packets encrypted with the handoff encryption key, between the second access point and the wireless terminal for immediate secured data transmission (secure data transmission *during the handoff without* perceivable interruption) [col. 2 lines 1-16, Fig. 1, 5, col. 6 lines 35-37].

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine Faccin with Choi provide immediate secure data transmission during the handoff without perceivable interruption, since one would have been motivated to provide security mobility between different cellular networks [Faccin, col. 1 lines 9-10].

Choi and Faccin do not expressively mention initiating authentication of the wireless terminal (re-authentication of the wireless terminal) and communicating the data packet for immediate secure data transmission *before the authentication of the wireless terminal is completed.*

Palekar teaches initiating authentication of the wireless terminal with an authentication server and communicating immediate secure data transmission before the authentication of the wireless terminal is completed [paragraph 0051].

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine Palekar with Choi and Faccin to establish the TLS

tunnel, since one would have been motivated to provide fast reconnect mechanism that allows wireless connections to be quickly resumed and to avoid service disruptions each time the mobile user connects to a different wireless access point [Palekar, paragraph 0010].

As per claim 2, the rejection of claim 1 is incorporated and Choi teaches: wherein the handoff encryption key is a handoff WEP (Wired Equivalent Privacy) key [Page 1, Introduction, Lines 11-14, page 6-7, 3.2, Fig. 5, 6]

As per claim 3, the rejection of claim 1 is incorporated and Choi teaches: wherein the handoff encryption key is generated by an authentication server [Page 1, Introduction, Lines 11-14, page 6-7, 3.2, Fig. 5, 6].

As per claim 4, the rejection of claim 1 is incorporated and Choi teaches: wherein the authentication server is an AAAH (Authentication, Authorization, and Accounting Home) server [Page 1, Introduction, Lines 15-20. Figure 5, "Home AAA Server"].

As per claim 5, the rejection of claim 1 is incorporated and Choi teaches: wherein the authentication server is an AAAF (Authentication, Authorization, and Accounting Foreign) server [Page 1, Introduction, Lines 15-20. Figure 5, "Gateway."].

As per claim 6, the rejection of claim 3 is incorporated and Choi teaches: wherein the handoff encryption key is generated according to IEEE 802.11 [Page 2, Introduction, Line 6].

As per claim 7, the rejection of claim 3 is incorporated and Choi teaches: transmitting the handoff encryption key to the first and second access points [Page 2, Introduction, Lines 17-19].

As per claim 8, the rejection of claim 7 is incorporated and Choi teaches: at the first access point transmitting the handoff encryption key to the wireless terminal [Page 7, §3.2, Lines 4-6].

As per claim 9, the rejection of claim 8 is incorporated and Choi teaches: at the second access point decrypting data from the wireless terminal with the handoff encryption key [page 6-7, 3.2, Fig. 5, 6].

As per claim 10, the rejection of claim 3 is incorporated and Choi teaches: communicating handoff authentication messages between the wireless terminal and the second access points [Page 7, §3.2, Lines 7-11].

As per claim 11, the rejection of claim 10 is incorporated and Choi teaches: encrypting the handoff authentication messages with the handoff encryption key [Page 7, §3.2, last sentence].

Choi discloses generation of the handoff was only shown within the Authentication, Authorization and Accounting (AAA) server(s). Despite, moving the key generation functionality from the AAA server(s), home or foreign, to the access points (AP) by either a transmission of the algorithm itself and its associated parameters or simply the parameters (assuming the algorithm is already present within the AP) is obvious to anyone of ordinary skill in the art at the time the invention was made because both logical units (AAA server(s) and the APs) are logically equivalent with regards to key generation. Whether the AAA server generates the handoff key to be transmitted to the APs or the AAA server gives the algorithm to the APs in order to generate the keys does not change the patentable weight of the invention. Further, the board has found that the limitation of the "metallic wrapping," which is really a lining of the tube, presents no novel or unexpected result over the metallic connections used in the references. Use of such a means of electrical connection in lieu of those used in the references solves no stated problem and would be an obvious matter of design choice within the skill of the art. The same situation arises in digital implementations when a system contains a plurality of logical units capable of the same functionality. Deciding whether one logical unit of a network system performs a specified functionality or another is an obvious matter of design choice. In other words, change of form or design

without change of function is no more than choice of design that, in absence of new or unobvious result, falls within ken of one having ordinary skill in art and will not sustain patentability. In re Launder, 42 CCPA 886, 222 F.2d 371, 105 USPQ 446 (1955); Flour City Architectural Metals v. Alpana Aluminum Products, Inc., 454 F. 2d 98, 172 USPQ 341 (8th Cir. 1972); National Connector Corp. v. Malco Manufacturing Co., 392 F.2d 766. 157 USPQ 401 (8th Cir.) cert. denied, 393 U.S. 923, 159 USPQ 799 (1968).

The claims are addressed individually in light of the reference teaching the same functionality of the instant application, and moving said functionality between the AAA server(s) and access points having been deemed obvious:

As per claim 12, the rejection of claim 1 is incorporated and Choi teaches: wherein the handoff encryption key is generated by the first and second access points as a function of common handoff encryption key generation information from an authentication server [Transposing functionality from one logical unit to another to forgo network communication is well known in the art and deemed obvious, and key generation by parameters (MAC, IP address, etcetera) is outlined within the taught use of IAPP (Page 2, Lines 11-15). Please see "IAPP Enhancement Protocol," §3.3-4, pages 343-344, for verification.].

As per claim 13, the rejection of claim 1 is incorporated and Choi teaches: at the second access point, determining whether a packet received is encrypted by the handoff encryption key [Page 7, §3.2, last sentence. Also Figure 6].

As per claim 14, the rejection of claim 13 is incorporated and Choi teaches: at the second access point, decrypting a packet encrypted by the handoff encryption key [Page 7, §3.2, Also Figure 6].

As per claim 15, the rejection of claim 1 is incorporated and Choi teaches: the first access point and the second access point receive a common handoff authentication key generation process from an authentication server [Page 6, §3.2, Lines 12-14].

As per claim 16, the rejection of claim 15 is incorporated and Choi teaches: providing a secret parameter to a handoff encryption key generator associated with the first access point; providing an open parameter to the handoff encryption key generator associated with the first access point; and generating the handoff encryption key as a function of the secret parameter and the open parameter [Key generation by parameters (MAC, IP address, etcetera) is outlined within the taught use of IAPP (Page 2, Lines 11-15). Please see "IAPP Enhancement Protocol," §3.3-4, pages 343-344, for verification].

As per claim 17, the rejection of claim 16 is incorporated and Choi teaches: wherein the secret parameter comprises information about the authentication server [Key generation by parameters (MAC, IP address, etcetera) is outlined within the taught use of IAPP (Page 2, Lines 11-15). Please see "IAPP Enhancement Protocol," §3.3-4, pages 343-344, for verification].

As per claim 18, the rejection of claim 17 is incorporated and Choi teaches: the secret parameter comprises ID information of the authentication server and at least one common parameter of the authentication server [Key generation by parameters (MAC, IP address, etcetera) is outlined within the taught use of IAPP (Page 2, Lines 11-15). Please see "IAPP Enhancement Protocol," §3.3-4, pages 343-344, for verification.].

As per claim 19, the rejection of claim 16 is incorporated and Choi teaches: wherein the open parameter comprises information about the first access point [Key generation by parameters (MAC, IP address, etcetera) is outlined within the taught use of IAPP (Page 2, Lines 11-15). Please see "IAPP Enhancement Protocol," §3.3-4, pages 343-344, for verification].

As per claim 20, the rejection of claim 16 is incorporated and Choi teaches: the open parameter comprises information about the wireless terminal [Key generation by parameters (MAC, IP address, etcetera) is outlined within the taught use of IAPP (Page 2, Lines 11-15). Please see "IAPP Enhancement Protocol," §3.3-4, pages 343-344, for verification].

As per claim 21, the rejection of claim 16 is incorporated and Choi teaches: the open parameter comprises the address of the first access point and the address of the wireless terminal [Key generation by parameters (MAC, IP address, etcetera) is outlined

within the taught use of IAPP (Page 2, Lines 11-15). Please see "IAPP Enhancement Protocol," §3.3-4, pages 343-344, for verification].

As per claim 22, the rejection of claim 16 is incorporated and Choi teaches: transmitting the handoff encryption key from the first access point to the wireless terminal [Page 7, §3.2, Lines 4-6].

As per claim 23, the rejection of claim 16 is incorporated and Choi teaches: at the wireless terminal, transmitting to the second access point data encrypted by the handoff encryption key [Figure 6, page 6-7 section 3.2].

As per claim 24, the rejection of claim 16 is incorporated and Choi teaches: at the second access point, obtaining the address of the first access point [Page 2, Introduction, Lines 11-14].

As per claim 25, the rejection of claim 16 is incorporated and Choi teaches: at the second access point, obtaining the address of the wireless terminal [Key generation by parameters (MAC, IP address, etcetera) is outlined within the taught use of IAPP (Page 2, Lines 11-15). Please see "§3.3-4, pages 343-344, Protocol" for verification. Please see "IAPP Enhancement Protocol," §3.3-4, pages 343-344, for verification].

As per claim 26, the rejection of claim 16 is incorporated and Choi teaches: at the second access point, deriving the handoff encryption key according to the key generation process [Key generation by parameters (MAC, IP address, etcetera) is outlined within the taught use of IAPP (Page 2, Lines 11-15). Please see "IAPP Enhancement Protocol," §3.3-4, pages 343-344, for verification].

As per claim 27, the rejection of claim 16 is incorporated and Choi teaches:
at the second access point, decrypting data from the wireless terminal with the handoff encryption key [Figure 6, page 6-7 section 3.2].

As per claim 28, Choi teaches: A wireless communication network comprising: an authentication server operable to generate and transmit a handoff encryption key; a first access point, receiving the handoff encryption key; and a second access point, receiving the handoff encryption key from the authentication server, at the time of handoff of a wireless terminal from the first access point to the second access point, decrypting the encrypted data from the wireless terminal [Page 1, Introduction, Lines 11-14 *and* Page 6-7, §3.2, Fig. 5, 6].
Choi teaches the authentication of the wireless terminal with an authentication server [Fig. 5].
Choi doesn't expressively mention decrypting encrypted data from the wireless terminal *before the authentication of the wireless terminal is completed.*

Faccin teaches at the time of a handoff of a wireless terminal from the first access point to the second access point, decrypting encrypted data from the wireless terminal (i.e. secure data transmission *during the handoff* without perceivable interruption) [col. 2 lines 1-16, Fig. 1, 5, col. 6 lines 13-29, 35-37].

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine Faccin with Choi provide immediate secure data transmission during the handoff without perceivable interruption, since one would have been motivated to provide security mobility between different cellular networks [Faccin, col. 1 lines 9-10].

Choi and Faccin do not expressively mention handling an authentication of the wireless terminal, at the time of a handoff of a wireless terminal from the fist access point to the second access point (re-authentication of the wireless terminal) while decrypting *before the authentication of the wireless terminal is completed*.

Palekar teaches handling an authentication of the wireless terminal, at the time of a handoff of a wireless terminal from the fist access point to the second access point (re-authentication of the wireless terminal) while decrypting the encrypted data *before the authentication of the wireless terminal is completed* [paragraph 0051].

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine Palekar with Choi and Faccin to establish the TLS tunnel, since one would have been motivated to provide fast reconnect mechanism that allows wireless connections to be quickly resumed and to avoid service disruptions

each time the mobile user connects to a different wireless access point [Palekar, paragraph 0010].

As per claim 29, the rejection of claim 28 is incorporated and it encompasses limitations that are similar to limitations of claim 2. Thus, it is rejected with the same rationale applied against claim 2 above.

As per claim 30, the rejection of claim 28 is incorporated and it encompasses limitations that are similar to limitations of claim 4. Thus, it is rejected with the same rationale applied against claim 4 above.

As per claim 31, the rejection of claim 28 is incorporated and it encompasses limitations that are similar to limitations of claim 5. Thus, it is rejected with the same rationale applied against claim 5 above.

As per claim 32, the rejection of claim 28 is incorporated and it encompasses limitations that are similar to limitations of claim 6. Thus, it is rejected with the same rationale applied against claim 6 above.

As per claim 33, the rejection of claim 28 is incorporated and it encompasses limitations that are similar to limitations of claim 10. Thus, it is rejected with the same rationale applied against claim 10 above.

As per claim 55, it encompasses limitations that are similar to limitations of claim 28. Thus, it is rejected with the same rationale applied against claim 28 above.

As per claim 64, the rejection of claim 3 is incorporated and Choi teaches: transmitting the handoff key to the first access point and the second access point, which is used to encrypt/decrypt the data during the handoff [Page 2, Introduction, Lines 17-19, Fig. 5]. Further, Faccin teaches the handoff encryption key is used during handing off from the first access point to the second access point [col. 6 lines 4-29, 35-37].

Double Patenting

The nonstatutory double patenting rejection is based on a judicially created doctrine grounded in public policy (a policy reflected in the statute) so as to prevent the unjustified or improper timewise extension of the "right to exclude" granted by a patent and to prevent possible harassment by multiple assignees. A nonstatutory obviousness-type double patenting rejection is appropriate where the conflicting claims are not identical, but at least one examined application claim is not patentably distinct from the reference claim(s) because the examined application claim is either anticipated by, or would have been obvious over, the reference claim(s). See, e.g., *In re Berg*, 140 F.3d 1428, 46 USPQ2d 1226 (Fed. Cir. 1998); *In re Goodman*, 11 F.3d 1046, 29 USPQ2d 2010 (Fed. Cir. 1993); *In re Longi*, 759 F.2d 887, 225 USPQ 645 (Fed. Cir. 1985); *In re Van Ornum*, 686 F.2d 937, 214 USPQ 761 (CCPA 1982); *In re Vogel*, 422 F.2d 438, 164 USPQ 619 (CCPA 1970); and In *re Thorington*, 418 F.2d 528, 163 USPQ 644 (CCPA 1969).

A timely filed terminal disclaimer in compliance with 37 CFR 1.321(c) or 1.321(d) may be used to overcome an actual or provisional rejection based on a nonstatutory

double patenting ground provided the conflicting application or patent either is shown to be commonly owned with this application, or claims an invention made as a result of activities undertaken within the scope of a joint research agreement.

Effective January 1, 1994, a registered attorney or agent of record may sign a terminal disclaimer. A terminal disclaimer signed by the assignee must fully comply with 37 CFR 3.73(b).

4. Claims 1-64 are provisionally rejected on the ground of nonstatutory obviousness-type double patenting as being unpatentable over claims 1-25 of copending Application No. 10/290,650. Although the conflicting claims are not identical, they are not patentably distinct from each other because both sets of claims are drawn to composing handoff encryption keys for two access points of an IEEE 802.11 standard network for fast handoff. Both sets of claims (instant application's claims 1-27 and copending application's claims 1-25) match in order they are presented using the most recent set of amended claims within the copending application (dated 10/27/2005).

This is a provisional obviousness-type double patenting rejection because the conflicting claims have not in fact been patented.

Response to Amendment

5. This written action is responding to the Request for Continued Examination (RCE) dated 12/19/2008. See new ground of rejection based on newly cited reference Palekar (US 2003/0226017) and previously cited prior art.

Examiner acknowledges the applicant's remark regarding the double patent rejection. Due to failure in submitting the terminal disclaimer for the provisional double patenting rejection, Examiner still maintains the Double patenting rejection.

Conclusion

6. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

Lee et al. (US 7158777) – Authentication method for fast handover in a wireless local area network

Rose (US 6771776) – Method and Apparatus for re-synchronization of a stream cipher during handoff

Maste (US 2004/0088550) – Network access management

Ala-Laurila et al (US 6587680) – Transfer of security association during a mobile terminal handover

Any inquiry concerning this communication or earlier communications from the examiner should be directed to NIRAV PATEL whose telephone number is (571)272-5936. The examiner can normally be reached on 8 am - 4:30 pm (M-F).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on 571-272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/N. P./
Examiner, Art Unit 2435
/Kimyen Vu/
Supervisory Patent Examiner, Art Unit 2435